Amendments to the Specification:

The following amendments to the Specification refer to the English translation of the international application as filed, and subsequently amended under Article 34. Copies of the English translation of the application as filed, and of the English translation of the claims as amended under Article 34 are provided herewith.

Immediately preceding paragraph [0001] on page 1, please insert the following Heading and Subheading:

--BACKGROUND OF THE INVENTION

1. Field of the Invention--

Immediately preceding paragraph [0002] on page 1, please insert the following Subheading:

--2. Description of the Related Art--

Immediately preceding paragraph [0008] on page 3, please insert the following Heading:

-- SUMMARY OF THE INVENTION--

Please replace paragraph [0008] with the following amended paragraph:

[0008] ~~The~~ An object of the invention is to provide a technique for particularly good protection of cryptographic calculations against attacks. ~~In particular,~~ A further object of the invention is to prevent attacks based on similar principles to the "Bellcore attack" described above. ~~should be prevented. In~~ Yet a further object in preferred configurations of the invention is that the protection according to the invention should advantageously cooperate with other protection methods.

Please replace paragraph [0009] with the following amended paragraph:

[0009] According to the ~~invention this object is~~ invention, the above objects are completely or partly achieved by a method for protected execution of a cryptographic calculation in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. ~~with the features of claim 1, a method for determining a key for a cryptographic calculation with the features of claim 12 , a computer program product as claimed in claim 14 and a portable data carrier as claimed in claim 15. The dependent claims define preferred configurations of the invention. The order in which the method steps are listed in the claims should not be interpreted as a limitation of the range of protection; rather, configurations of the invention are provided, in which these method steps are executed completely or partly in a different order or completely or partly parallel or completely or partly interleaved.~~

Please insert the following new paragraphs [0009.1], [0009.2], [0009.3], and [0009.4] immediately following amended paragraph [0009]:

[0009.1] Further according to the invention, the above objects are completely or partly achieved by a method for determining a key for a cryptographic calculation with at least two key parameters, the key being adapted to be used in a method for protected execution of a cryptographic calculation wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

[0009.2] Further according to the invention, the above objects are completely or partly achieved by a computer program product which has program commands to cause a processor to execute a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

[0009.3] Further according to the invention, the above objects are completely or partly achieved by a portable data carrier set up for executing a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

[0009.4] The order in which the method steps are listed in the claims should not be interpreted as a limitation of the range of protection; rather, configurations of the invention are provided, in which these method steps are executed completely or partly in a different order or completely or partly parallel or completely or partly interleaved.

Immediately preceding paragraph [0020] on page 6, please insert the following Heading:

--BRIEF DESCRIPTION OF THE DRAWINGS--

Immediately preceding paragraph [0025] on page 6, please insert the following Heading:

--DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION--

Please insert the following new paragraph [0054] immediately following paragraph [0053] on page 16 of the specification as filed:

[0054] The particulars contained in the above description of sample embodiments should not be construed as limitations of the scope of the invention, but rather as exemplifications of preferred embodiments thereof. Accordingly, the scope of the invention should be determined not by the embodiments illustrated, but by the appended claims and their legal equivalents.

Please insert the following line immediately following new paragraph [0054] on page 16:

What is claimed is: